

**IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT**

No. 17-11271

United States Court of Appeals
Fifth Circuit

FILED

October 1, 2018

Lyle W. Cayce
Clerk

UNITED STATES OF AMERICA,

Plaintiff - Appellee

v.

SEBASTIAN CONTRERAS,

Defendant - Appellant

Appeal from the United States District Court
for the Northern District of Texas

Before STEWART, Chief Judge, and WIENER and HIGGINSON, Circuit Judges.

STEPHEN A. HIGGINSON, Circuit Judge:

On April 4, 2017, federal agents executed a search warrant for child pornography at the home of Defendant-Appellant Sebastian Contreras. Agents retrieved, among other items, Contreras's laptop and external hard drive, on which Contreras had downloaded multiple videos depicting the sexual abuse of infants and minor children. Contreras conditionally pleaded guilty to two counts of receipt of child pornography, reserving the right to appeal the district court's denial of his motion to suppress. On direct appeal, Contreras contends that the search of his home was not supported by probable cause. We AFFIRM.

No. 17-11271

FACTS AND PROCEEDINGS

On April 15, 2016, and again on April 17, 2016, an undercover Homeland Security Investigations (“HSI”) agent saw that user “alex2smith13” had uploaded sexually graphic images of young children to a group chat on Kik, a mobile messaging application. Also on April 15, 2016, the Northern District of Florida issued a grand jury subpoena to Kik, Inc. Kik turned over records showing that “alex2smith13” had accessed Kik from IP address 108.37.82.115. That IP address, the government found, had been ported by internet service provider Verizon Wireless to Frontier Communications. On May 13, 2016, the Northern District of Florida issued a grand jury subpoena to Frontier. Frontier responded that the IP address was registered to customer Saul Contreras (Contreras’s father) at a residential address in Brownwood, Texas. Local law enforcement confirmed in November 2016 and again in March 2017 that the Contreras family continued to live at that Brownwood address.

On March 29, 2017, HSI agent Sean Dunagan applied for and was issued a search warrant for the Contreras home extending to images of child pornography stored on cell phones, computers, and computer hardware. Agent Dunagan’s affidavit in support recounted the facts of the initial investigation and explained that (1) modern internet-connected computers and cell phones have made it possible to share child pornography securely and anonymously; (2) an individual can use a cell phone in tandem with a computer to transfer, store, or back up child pornography files; (3) people who view child pornography typically store the materials for many years in the privacy and security of their own homes; and (4) forensic experts can generally recover evidence of child pornography on a computer even if files were stored remotely (e.g., on Dropbox) or deleted. Dunagan based these statements in part on his experience, training, and background as a federal criminal investigator since 2008 with prior experience in investigating the sexual exploitation of children.

No. 17-11271

At Dunagan's request, an Assistant U.S. Attorney reviewed the search warrant application before it was submitted to the magistrate judge. Federal agents executed the warrant on April 4, 2017 and seized, among other objects, Contreras's personal computer and external hard drive.

A two-count indictment charging Contreras with transportation of child pornography was filed on April 12, 2017, and a seven-count superseding indictment charging him with receipt as well as transportation was filed on May 17, 2017. Contreras moved to suppress the evidence seized in the search, arguing that Dunagan's affidavit in support of the warrant made material omissions, the affidavit on its face did not establish probable cause, and the government needed a warrant to obtain Frontier's records connecting the 108.37.82.115 IP address with the Contreras family residence. The district court held an evidentiary hearing and denied the motion after finding that the affidavit was truthful, contained no material omissions, and established probable cause. Contreras reserved the right to challenge the district court's ruling and conditionally pleaded guilty to two counts of Receipt of a Visual Depiction of a Minor Engaging in Sexually Explicit Conduct, in violation of 18 U.S.C. § 2252(a)(2). The district court sentenced Contreras to 168 months of imprisonment on each count, to run concurrently, and to a ten-year term of supervised release. Contreras timely appealed.

DISCUSSION

On appeal, Contreras argues that evidence from the April 2017 search should be suppressed because (1) the government violated Contreras's reasonable expectation of privacy in the family address when it obtained

No. 17-11271

Frontier's records without a warrant and (2) Dunagan's affidavit on its face failed to establish probable cause for the search warrant.¹

The district court's factual findings are reviewed for clear error and its conclusions of law are reviewed *de novo*. *United States v. Payne*, 341 F.3d 393, 399 (5th Cir. 2003). We uphold a district court's denial of a suppression motion "if there is any reasonable view of the evidence to support it." *United States v. Michelletti*, 13 F.3d 838, 841 (5th Cir. 1994) (en banc) (quoting *United States v. Register*, 931 F.2d 308, 312 (5th Cir. 1991)). All evidence is viewed in the light most favorable to the party who prevailed below—here, the government. *United States v. Massi*, 761 F.3d 512, 520 (5th Cir. 2014).

I. Contreras had no reasonable expectation of privacy in Frontier's records

We first address whether Contreras had a reasonable expectation of privacy in the family address as contained in Frontier's records. In a series of precedents dating back to 1976, the Supreme Court has found that "a person has no legitimate expectation of privacy in information . . . voluntarily turn[ed] over to third parties," "even if the information is revealed on the assumption that it will be used only for a limited purpose." *Carpenter v. United States*, 138 S. Ct. 2206, 2216 (2018) (quoting *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979) and *United States v. Miller*, 425 U.S. 435, 443 (1976)). The third-party doctrine has limits: in *Carpenter*, the Supreme Court declined to extend the rule to cell-site records that convey "a detailed and comprehensive record of [a] person's movements." *Id.* at 2217. But the third-party doctrine continues to apply to "business records that might incidentally reveal location information," including telephone numbers and bank records. *Id.* at 2220.

¹ Contreras affirmatively waives his argument that Dunagan acted in bad faith by submitting an affidavit with material omissions.

No. 17-11271

The information at issue here falls comfortably within the scope of the third-party doctrine. Frontier's records revealed only that the IP address was associated with the Contreras's Brownwood residence. They had no bearing on any person's day-to-day movement. Contreras lacked a reasonable expectation of privacy in that information.

II. The good faith exception applies

We next take up Contreras's contention that suppression is appropriate because the search warrant issued without probable cause. When a search warrant is involved, this court first determines whether the good faith exception to the exclusionary rule applies. *United States v. Froman*, 355 F.3d 882, 888 (5th Cir. 2004). The good faith exception provides that "evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant" typically should not be excluded. *United States v. Leon*, 468 U.S. 897, 922 (1984).

If the good faith exception does apply, we may affirm the district court's denial of the motion to suppress without reaching the question of probable cause. *United States v. Cherna*, 184 F.3d 403, 407 (5th Cir. 1999); *see also United States v. Craig*, 861 F.2d 818, 820 (5th Cir. 1988) ("Principles of judicial restraint and precedent dictate that, in most cases, we should not reach the probable cause issue if a decision on the admissibility of the evidence under the good-faith exception of *Leon* will resolve the matter."). But even where the good faith exception alone would be dispositive, we may review the district court's probable cause determination if the appellant raises "a novel question of law whose resolution is necessary to guide future action by law enforcement officers and magistrates." *United States v. Maggitt*, 778 F.2d 1029, 1033 (5th Cir. 1985) (quoting *Illinois v. Gates*, 462 U.S. 213, 264 (1983) (White, J., concurring)).

No. 17-11271

Contreras argues that his appeal raises novel questions of law concerning probable cause in the digital era, but he fails to address the first step in our suppression analysis: whether it was objectively reasonable for officers to rely on the search warrant. To the extent that Contreras's probable cause arguments can be recast as challenges to objective reasonableness, he fails to show that the good faith exception should not apply.

“We have identified four situations in which the good faith exception does not apply: (1) when the issuing magistrate was misled by information in an affidavit that the affiant knew or reasonably should have known was false; (2) when the issuing magistrate wholly abandoned his judicial role; (3) when the warrant affidavit is so lacking in indicia of probable cause as to render official belief in its existence unreasonable; and (4) when the warrant is so facially deficient in failing to particularize the place to be searched or the things to be seized that executing officers cannot reasonably presume it to be valid.” *United States v. Woerner*, 709 F.3d 527, 533–34 (5th Cir. 2013). Contreras's probable cause arguments are relevant to the third circumstance, whether the warrant affidavit was so devoid of indicia of probable cause that reliance on the warrant was objectively unreasonable.

Contreras first contends that uploading two images of child pornography over the course of a few days from a cell phone connected to a residential WiFi network does not establish probable cause to search that residence for evidence of child pornography, because the images could conceivably have been uploaded by a temporary guest or an unauthorized neighbor. That may be, but probable cause does not demand more than a “fair probability” on which a reasonable person would act. *Florida v. Harris*, 568 U.S. 237, 244 (2013). There was at least a fair probability that “alex2smith13” actually lived at the Contreras home, and our court, as well as others across the country, has found probable cause to search a residence based on just one or two uploads of child

No. 17-11271

pornography. *See, e.g., United States v. Perez*, 484 F.3d 735, 740 (5th Cir. 2007) (single upload); *United States v. Vosburgh*, 602 F.3d 512, 526 (3d Cir. 2010) (single download); *United States v. Hinojosa*, 606 F.3d 875, 878, 885 (6th Cir. 2010) (two chat sessions over the course of ten days). As a result, Contreras fails to show that the facts listed in the affidavit lacked indicia of probable cause.

Contreras next argues that the information in the affidavit was stale because HSI observed two Kik uploads in April 2016 but did not seek a warrant until March 2017. Certainly, probable cause must “exist at the time the warrant issues.” *United States v. McKeever*, 5 F.3d 863, 866 (5th Cir. 1993). But there is no bright-line test, *United States v. Allen*, 625 F.3d 830, 842 (5th Cir. 2010), and information is less likely to be stale if “the evidence sought is of the sort that can reasonably be expected to be kept for long periods of time in the place to be searched,” *Craig*, 861 F.2d at 822–23. Here, Dunagan attested that evidence in child pornography cases may be kept for years because people who collect child pornography typically maintain those materials for a long time, and forensic experts can frequently recover evidence of deleted files. Those assertions were offered alongside “specific facts” linking the Contreras residence to uploads of child pornography. *See United States v. Broussard*, 80 F.3d 1025, 1035 (5th Cir. 1996). Under these circumstances, the year-long interval between Contreras’s Kik posts and the government’s application for a search warrant did not render reliance on the search warrant objectively unreasonable.

Finally, Contreras contends that because Kik is a messaging application for cell phones only, there was no probable cause to search for and seize computers or other objects. This argument is unpersuasive. Dunagan’s affidavit noted that cell phones can easily be used in conjunction with computers to transfer, view, back up, or store child pornography images.

No. 17-11271

Since we conclude that the good faith exception applies and is dispositive, we need not consider whether the magistrate judge had probable cause to issue the warrant. That determination would turn only on “relatively well-settled” Fourth Amendment law. *Maggitt*, 778 F.2d at 1033.

CONCLUSION

The district court is AFFIRMED.